

# AN ELEMENTARY INDUCTIVE PROOF THAT $AB = I$ IMPLIES $BA = I$ FOR MATRICES

J. M. ALMIRA

**ABSTRACT.** In this note we give an elementary demonstration of the fact that  $AB = I_n$  implies  $BA = I_n$  for square matrices  $A, B$  with coefficients in a field  $\mathbb{K}$ .

## 1. INTRODUCTION

Let  $\mathbb{K}$  be a division ring and  $M_n(\mathbb{K})$  be the ring of square matrices of order  $n$  with coefficients in  $\mathbb{K}$ . Let us denote by  $I_n$  the identity matrix of order  $n$ , which is the unit element of  $M_n(\mathbb{K})$ . A very basic important fact about matrices is that they are non-commuting objects, even if  $\mathbb{K}$  is commutative. This is important because matrices naturally appear in many applications where their non-commutativity is a key ingredient (I am thinking about Quantum Mechanics but there are thousands of other examples for this claim). Thus, from the simple assumption that  $AB = I_n$  for two square matrices  $A, B \in M_n(\mathbb{K})$ , it is not self evident that  $BA = I_n$  since  $AB$  and  $BA$  may differ. Thus, when introducing invertible linear maps or invertible matrices in a Linear Algebra introductory course, it is usual to force the equalities  $AB = BA = I_n$  to tell that matrices  $A, B$  are invertible and  $B = A^{-1}$  (see, e.g., [3, Section 2.3], [1, page 214], and [4, page 25]. In spite of the strong differences between all these books, the same path for a definition of invertible matrices is adopted). On the other hand, the following result is well known and classic [5, page 101] (see also [2, page 14]):

**Theorem 1.1.** *If  $\mathbb{K}$  is a field and  $A, B \in M_n(\mathbb{K})$ , then  $AB = I_n$  implies  $BA = I_n$ .*

Hence, for any field  $\mathbb{K}$  and any natural number  $n$ , we can claim that a square matrix  $A \in M_n(\mathbb{K})$  is invertible (with inverse  $B$ ) if and only if  $AB = I_n$ .

In this note we give an elementary demonstration of Theorem 1.1. By “elementary” we mean that our proof follows from the very definitions of matrix and product of a matrix, with no extra help of more sophisticated results, as the use of dimensions of vector spaces or other ring-theoretical properties, as being Noetherian. The proof is also elementary in the sense that it relies on the concept and properties of the so called elementary operations on matrices. Finally, and no less important, this proof can be faced by any good student of a first year course in Mathematics, Physics or Engineering.

## 2. THE PROOF

For our proof it is important to know how Gaussian row-reduction elimination process works. Concretely, it is important to observe that, for the elementary matrices associated to elementary operations a direct concept of inverse can be introduced. By this I mean that, for example, if  $E_{i,j}$  denotes the matrix which results from interchanging the  $i$ -th and  $j$ -th rows of the identity matrix  $I_n$ , then it is clear that  $E_{i,j}E_{i,j} = I_n$  so that we can define  $E_{i,j}^{-1} = E_{i,j}$ . Similar considerations can be done for the other types of elementary matrices: the elementary operation that reverses

---

2010 *Mathematics Subject Classification.* 15A03, 15A09.

*Key words and phrases.* Matrices, Linear Algebra, Abstract Algebra.

the work done by a given elementary operation is well known, is unique, and can be used to define the inverse matrix of the elementary matrix associated to the given elementary operation. Thus, for every elementary matrix  $E$  we perfectly know what we mean by  $E^{-1}$ . Moreover, we also need to use the following known fact: when we perform an elementary operation whose associated elementary matrix is  $E$  to a given matrix  $A$ , the new matrix we get is  $A^* = EA$ .

**Lemma 2.1.** *Let  $A, B \in M_n(\mathbb{K})$  and assume  $A = \begin{bmatrix} \alpha & v^t \\ u & \tilde{A} \end{bmatrix}$  and  $B = \begin{bmatrix} \beta & w^t \\ h & \tilde{B} \end{bmatrix}$ . Then*

$$AB = \begin{bmatrix} \alpha\beta + v^th & \alpha w^t + v^t\tilde{B} \\ \beta u + \tilde{A}h & uw^t + \tilde{A}\tilde{B} \end{bmatrix}$$

*Proof.* This is a direct computation.  $\square$

**Lemma 2.2.** *Assume that  $A, B \in M_n(\mathbb{K})$  satisfy  $AB = I_n$ . If  $Ax = 0$ , then  $x = 0$ .*

*Proof.* We proceed by induction on  $n$ . The result trivially holds for  $n = 1$ , since  $AB = 1$  implies  $A \neq 0$  for scalars. Hence  $Ax = 0$  implies  $x = 0$ . Assume  $n > 1$ , decompose  $A, B$  as the formulas given in Lemma 2.1 and impose  $AB = I_n$ . We decompose our proof in two cases:

**Case 1.**  $A = \begin{bmatrix} 0 & v^t \\ 0 & \tilde{A} \end{bmatrix}$ .

In this case, we have that  $\alpha = 0$  and  $u = 0$ , so that Lemma 2.1 tell us that

$$I_n = AB = \begin{bmatrix} v^th & v^t\tilde{B} \\ \tilde{A}h & \tilde{A}\tilde{B} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & I_{n-1} \end{bmatrix}$$

It follows that  $\tilde{A}\tilde{B} = I_{n-1}$  and  $\tilde{A}h = 0$ ,  $v^th = 1$ . Now, the induction hypothesis lead us to conclude that  $h = 0$ , which contradicts  $v^th = 1$ . Hence  $AB = I_n$  can't hold if the first column of  $A$  contains only zeros.

**Case 2.** The first column of  $A$  is not identically zero.

In this case we can perform elementary operations with associated elementary matrices  $E_1, \dots, E_t$  to transform the matrix  $A$  into a matrix  $A^*$  of the form  $A^* = E_1 \cdots E_t A = \begin{bmatrix} 1 & (v^*)^t \\ 0 & \tilde{A}^* \end{bmatrix}$ .

Then  $B^* = BE_t^{-1} \cdots E_1^{-1}$  satisfies

$$(1) \quad A^*B^* = E_1 \cdots E_t ABE_t^{-1} \cdots E_1^{-1} = E_1 \cdots E_t \cdot E_t^{-1} \cdots E_1^{-1} = I_n.$$

Let us write  $B^* = \begin{bmatrix} \beta^* & (w^*)^t \\ h^* & \tilde{B}^* \end{bmatrix}$ . Then

$$(2) \quad \begin{aligned} \begin{bmatrix} 1 & 0 \\ 0 & I_{n-1} \end{bmatrix} &= I_n = A^*B^* = \begin{bmatrix} 1 & (v^*)^t \\ 0 & \tilde{A}^* \end{bmatrix} \begin{bmatrix} \beta^* & (w^*)^t \\ h^* & \tilde{B}^* \end{bmatrix} \\ &= \begin{bmatrix} \beta^* + (v^*)^th^* & (w^*)^t + (v^*)^t\tilde{B}^* \\ \tilde{A}^*h^* & \tilde{A}^*\tilde{B}^* \end{bmatrix} \end{aligned}$$

In particular, we have that  $\tilde{A}^*\tilde{B}^* = I_{n-1}$ , and  $\tilde{A}^*h^* = 0$ , so that the induction hypothesis implies that  $h^* = 0$  and the identity  $\beta^* + (v^*)^th^* = 1$  is reduced to  $\beta^* = 1$ . Assume that  $Ax = 0$ , with  $x^t = [x_1, x^*]$ . Then  $A^*x = E_1 \cdots E_t Ax = E_1 \cdots E_t 0 = 0$ . Hence

$$0 = A^*x = A^* \begin{bmatrix} x_1 \\ x^* \end{bmatrix} = \begin{bmatrix} 1 & (v^*)^t \\ 0 & \tilde{A}^* \end{bmatrix} \begin{bmatrix} x_1 \\ x^* \end{bmatrix} = \begin{bmatrix} x_1 + (v^*)^tx^* \\ \tilde{A}^*x^* \end{bmatrix}$$

It follows that  $\tilde{A}^*x^* = 0$  and the induction hypothesis implies that  $x^* = 0$ . Hence  $0 = x_1 + (v^*)^tx^* = x_1$ . This proves  $x = 0$ .  $\square$

**Lemma 2.3.** *If  $AB = I_n$  then the first column of  $A$  can't be the zero vector.*

*Proof.* If the first column of  $A$  vanishes, then  $Ae_1 = 0$ , where  $e_1$  denotes the vector  $[1, 0, \dots, 0]^t \in \mathbb{K}^n$ , which is not the zero vector. This contradicts Lemma 2.2.  $\square$

Now we can demonstrate the main result of this paper:

*Proof of Theorem 1.1.* It follows from Lemma 2.3 that the first column of  $A$  does not vanish identically. Hence we can proceed as in the proof of Case 2 in Lemma 2.2 to construct the matrices  $A^* = E_1 \cdots E_t A = \begin{bmatrix} 1 & (v^*)^t \\ 0 & \widetilde{A^*} \end{bmatrix}$  and  $B^* = BE_t^{-1} \cdots E_1^{-1}$ . Obviously, these matrices satisfy (1) and (2). Moreover,

$$B^* A^* = BE_t^{-1} \cdots E_1^{-1} E_1 \cdots E_t A = BA.$$

In particular, (2) leads to  $\widetilde{A^*} \widetilde{B^*} = I_{n-1}$ , and the induction hypothesis implies that  $\widetilde{B^*} \widetilde{A^*} = I_{n-1}$  too. Now Lemma 2.2 and the equality  $\widetilde{A^*} h^* = 0$  imply that  $h^* = 0$ . Using this fact on the identity  $\beta^* + (v^*)^t h^* = 1$  leads to  $\beta^* = 1$ . Furthermore, we also have that

$$(3) \quad (w^*)^t + (v^*)^t \widetilde{B^*} = 0.$$

Let us now consider the product  $BA$ :

$$\begin{aligned} BA &= B^* A^* = \begin{bmatrix} 1 & (w^*)^t \\ 0 & \widetilde{B^*} \end{bmatrix} \begin{bmatrix} 1 & (v^*)^t \\ 0 & \widetilde{A^*} \end{bmatrix} \\ &= \begin{bmatrix} 1 & (v^*)^t + (w^*)^t \widetilde{A^*} \\ 0 & \widetilde{B^*} \widetilde{A^*} \end{bmatrix} \\ &= \begin{bmatrix} 1 & (v^*)^t + (w^*)^t \widetilde{A^*} \\ 0 & I_{n-1} \end{bmatrix}. \end{aligned}$$

It follows from (3) that

$$\begin{aligned} 0 &= ((w^*)^t + (v^*)^t \widetilde{B^*}) \widetilde{A^*} \\ &= (w^*)^t \widetilde{A^*} + (v^*)^t \widetilde{B^*} \widetilde{A^*} \\ &= (w^*)^t \widetilde{A^*} + (v^*)^t I_{n-1} \\ &= (v^*)^t + (w^*)^t \widetilde{A^*}, \end{aligned}$$

which implies that

$$BA = B^* A^* = \begin{bmatrix} 1 & 0 \\ 0 & I_{n-1} \end{bmatrix} = I_n.$$

This ends the proof.  $\square$

### 3. OTHER PROOFS

**3.1. A proof based on dimension of vector spaces.** By fixing a basis of the vector space  $\mathbb{K}^n$ , we can identify in the natural way  $M_n(\mathbb{K})$  with the vector space  $\text{End}(\mathbb{K}^n)$ . Then the range of a matrix  $A$  coincides with the dimension of the associated image space (which is spanned by columns of  $A$ ). From  $AB = I_n$  we conclude that  $AB$  has range  $n$  and, consequently, the range of  $B$  must be also  $n$  since, otherwise, the image space of  $AB$  would be spanned by a set of at most  $n - 1$  vectors (just take a set of  $n - 1$  vectors spanning the range of  $B$  and apply  $A$  to these concrete vectors). Now,  $B = BI_n = B(AB) = (BA)B$  implies  $(I_n - BA)B = 0$  and, since  $B$  has full rank,  $I_n - BA$  is the null map. This means  $BA = I_n$  and proves Theorem 1.1.

**3.2. A proof based on Noetherian property.** We take this proof from the well known abstract algebra website [6]. A ring  $R$  is called Dedekind-finite if for all  $a, b \in R$ , the identity  $ab = 1$  implies  $ba = 1$ .

**Theorem 3.1.** *Every (left or right) Noetherian ring  $R$  is Dedekind-finite.*

*Proof.* We will assume that  $R$  is left Noetherian. Suppose that  $ab = 1$  for some  $a, b \in R$ . Define the map  $f : R \rightarrow R$  by  $f(r) = rb$ . Clearly  $f$  is an  $R$ -module homomorphism and is onto because  $f(ra) = (ra)b = r(ab) = r$ , for all  $r \in R$ . Now we have an ascending chain of left ideals of  $R$

$$\ker f \subseteq \ker f^2 \subseteq \cdots$$

Since  $R$  is left Noetherian, this chain stabilizes at some point, which means that there exists some  $n$  such that  $\ker f^n = \ker f^{n+1}$ . Clearly  $f^n$  is onto because  $f$  is onto. Thus  $f^n(c) = ba - 1$  for some  $c \in R$ . Then  $f^{n+1}(c) = f(ba - 1) = (ba - 1)b = b(ab) - b = 0$ . Hence  $c \in \ker f^{n+1} = \ker f^n$  and therefore  $ba - 1 = f^n(c) = 0$ . This ends the proof.  $\square$

**Theorem 3.2.** *Let  $\mathbb{K}$  be a field and let  $R$  be a finite dimensional  $\mathbb{K}$ -algebra. Then  $R$  is Dedekind-finite.*

*Proof.* Every left ideal of  $R$  is a  $\mathbb{K}$ -vector subspace of  $R$  and thus, since  $\dim_{\mathbb{K}} R < \infty$ , any ascending chain of left ideals of  $R$  will stop at some point. So  $R$  is left Noetherian and thus, it is also Dedekind-finite.  $\square$

Now Theorem 1.1 follows as a corollary of Theorem 3.2 since  $M_n(\mathbb{K})$  is a finite dimensional  $\mathbb{K}$ -algebra. What is more, we can conclude that  $M_n(R)$  is Dedekind-finite for any commutative domain  $R$  because  $M_n(R)$  is a subring of  $M_n(\hat{R})$ , where  $\hat{R}$  is the quotient field of  $R$ .

#### 4. THE RESULT DOES NOT HOLD FOR OPERATORS ON INFINITE DIMENSIONAL VECTOR SPACES

Let  $V$  be any infinite dimensional vector space over the field  $\mathbb{K}$ . Let  $\{e_k\}_{k=1}^{\infty}$  be a linear independent set in  $V$  and consider  $\beta = \{e_k\}_{k=1}^{\infty} \cup \{w_j\}_{j \in J}$  a basis of  $V$  which contains  $e_k$  for all  $k$ . We introduce the linear maps  $A, B \in \text{End}(V)$  defined by

$$\begin{cases} A(e_k) = e_{k+1} & \text{for all } k = 1, 2, \dots \\ A(w_j) = w_j & \text{for all } j \in J \end{cases}$$

and

$$\begin{cases} B(e_1) = 0 \\ B(e_k) = e_{k-1} & \text{for all } k = 2, 3, \dots \\ B(w_j) = w_j & \text{for all } j \in J \end{cases}$$

Then  $BA = 1_d$  and  $ABe_1 = A0 = 0$ , so that  $AB \neq 1_d$ . This, jointly with Theorem 1.1, proves the following

**Theorem 4.1.** *Let  $V$  be a vector space. Then  $\text{End}(V)$  is Dedekind-finite iff  $\dim V < \infty$ .*

#### REFERENCES

1. S. AXLER, *Linear Algebra done right*, Springer, 1996.
2. R. A. HORN AND C. R. JOHNSON, *Matrix Analysis: Second Edition*, Cambridge University Press, 2012.
3. W.K. NICHOLSON, *Linear Algebra with applications*, McGraw Hill Higher Education; 6th Revised edition edition (2009)
4. S. TREIL, *Linear Algebra done wrong*, A textbook for an honors linear algebra course, free available at <https://www.math.brown.edu/~treil/papers/LADW/LADW.html>
5. B.L. VAN DER WAERDEN, *Modern Algebra, Volume II*, Frederic Ungar Publishing Co., 1950.
6. <https://ysharifi.wordpress.com/2010/09/17/dedekind-finite-rings/>

DEPARTAMENTO DE MATEMÁTICAS, UNIVERSIDAD DE JAÉN, E.P.S. LINARES, CAMPUS CIENTÍFICO TECNOLÓGICO DE LINARES, CINTURÓN SUR S/N, 23700 LINARES, SPAIN

*E-mail address:* `jmalmira@ujaen.es`